Homework 5

Mark Schulist

1)

1.a)

$$f(x) = x^5 + x^4 + 1 = 0 \bmod 243 \tag{1}$$

We know that $243 = 3^5$.

$$f(x) = x^5 + x^4 + 1 = 0 \bmod 3 \tag{2}$$

$f(1)$ is the only solution.

$$\begin{aligned} f'(x) &= 5x^4 + 4x^3 \\ f'(1) &= 9 = 0 \bmod 3 \end{aligned} \tag{3}$$

So could all be solutions are none be solutions.

$$f(1) = 3 \neq 0 \bmod 9 \tag{4}$$

So none are solutions. Hence there is no solution to $f(x) = 0 \bmod 243$.

1.b)

$$f(x) = x^3 + x + 87 = 0 \bmod 125 \tag{5}$$

We know that $125 = 5^3$.

$f(4) = 0 \bmod 5$ is only solution, so 4 is a solution mod 5.

$$\begin{aligned} f'(x) &= 3x^2 + 1 \\ f'(4) &= 49 = 4 \bmod 5 \end{aligned} \tag{6}$$

So there is a unique lift.

$$\begin{aligned} t &= -f'(4)^{-1} \frac{f(4)}{5} \bmod 5 \\ t &= -4 \cdot 31 \bmod 5 \\ t &= 1 \bmod 5 \end{aligned} \tag{7}$$

$$a' = 4 + 5 = 9 \tag{8}$$

Now let $a = 9$, we are in mod 25.

$$f'(9) = 244 = 4 \bmod 5 \tag{9}$$

$$t = -4 \frac{f(9)}{25} = -4 \cdot 33 = -132 = -7 = 18 \bmod 25 \tag{10}$$

$$a' = 9 + 18 \cdot 25 = 459 = 84 \bmod 125 \tag{11}$$

So $x = 84$ is a solution mod 125.

1.c)

$$x^3 - x^2 = 0 \bmod 16 \tag{12}$$

Mod 4, we can see that $f(0) = f(1) = f(2) = 0 \bmod 4$. So there are 3 solutions mod 4.

Start with 0.

$$\begin{aligned} f'(0) &= 0 \\ f(0) &= 0 \end{aligned} \tag{13}$$

So all are lifts. $a' = 0, 4, 8, 12$.

Now do 1.

$$f'(1) = 1 \tag{14}$$

$$\begin{aligned} t &= -1 \cdot \frac{f(1)}{4} \bmod 4 \\ &= 0 \end{aligned} \tag{15}$$

So $a' = a + 0 = 1$.

Now do 2.

$$f'(2) = 8 = 0 \bmod 4 \tag{16}$$

$a' = a = 2$. $f(2) = 4 \bmod 16$, so none are solutions.

So $x = 0, 1, 4, 8, 12$ are solutions!

2)

2.a)

$$x^3 - x = 0 \bmod 48 \tag{17}$$

$x^3 - x^2 = 0 \bmod 16$ has 5 solutions.

$x^3 - x^2 = 0 \bmod 3$ has 2 solutions.

So we have 10 solutions in all.

2.b)

$$x^3 + x + 87 = 0 \bmod 1000 \tag{18}$$

$x^3 + x + 87 = 0 \bmod 125$ has one solution.

$x^3 + x + 1 = 2x + 1 = 1 = 0 \bmod 2$ has no solutions!

So there are no solutions overall!

3)

All we know is that $x^p = x \bmod p$.

3.a)

$$\begin{aligned} x^7 &= x \bmod 7 \\ x^{11} &= x^5 \bmod 7 \end{aligned} \tag{19}$$

$$\begin{aligned} x^7 &= x \bmod 7 \\ x^8 &= x^2 \bmod 7 \end{aligned} \tag{20}$$

So $x^{11} + x^8 + 5 = 0 \bmod 7$ is same as $x^5 + x^2 + 5 = 0 \bmod 7$.

3.b)

$$\begin{aligned} x^7 &= x \bmod 7 \\ x^{20} &= x^{14} \bmod 7 \end{aligned} \tag{21}$$

$$\begin{aligned} x^7 &= x \bmod 7 \\ x^{14} &= x^8 \bmod 7 \end{aligned} \tag{22}$$

And we know that $x^8 = x^2 \bmod 7$ from above problem.

$$\begin{aligned} x^7 &= x \bmod 7 \\ x^{13} &= x^7 = x \bmod 7 \end{aligned} \tag{23}$$

So $x^{20} + x^{13} + x^7 + x = 2 \bmod 7$ is the same as $x^2 + x + x + x = x^2 + 3x = 2 \bmod 7$.

4)

p is prime, $d \in \mathbb{N}$, $d \mid p - 1$.

We want to show that $f(x) = a^p - 1 \bmod p^n$ has d solutions mod p. We know that $0 \leq d \leq p - 1$.

$$f'(x) = dx^{d-1} \bmod p \tag{24}$$

Now our goal is to show that $f'(x) \neq 0$ for any $x \in \mathbb{Z}/p\mathbb{Z}$.

We know that $d \neq 0$, so the only way that $f'(x) = 0$ is if $h(x) = x^{d-1} = 0 \bmod p$ (as we are working mod p, and $0 \notin (\mathbb{Z}/p\mathbb{Z})^\times$, and is only element that is not a unit).

Now we show that $h(x) \neq 0 \bmod p$ for any $x \in \mathbb{Z}/p\mathbb{Z}$.

$x^{d-1} = 0 \bmod p$ means that $x^{d-1} = pk$ for some $k \in \mathbb{Z}$. But the only possible value that can divide the RHS is p, but $x \neq p$ as $p = 0 \bmod p$, and we know that $x \neq 0$. Hence there is no $x \in \mathbb{Z}/p\mathbb{Z}$ (besides 0) which can make $x^{d-1} = 0$. Therefore we have shown that $h(x) \neq 0$ for any $x \in \mathbb{Z}/p\mathbb{Z}$.

So now we know that there must be unique lifts, which means that all $d \in \mathbb{Z}/p\mathbb{Z}$ get lifted once so there are always d solutions at each level (each n of p^n, and we know there are d solutions in $\mathbb{Z}/p\mathbb{Z}$ by the theorem from class).

5)

p is prime.

5.a)

f is a monic polynomial in $\mathbb{Z}/p\mathbb{Z}$ and has exactly n roots in $\mathbb{Z}/p\mathbb{Z}$. Show that f can be factored as $f(x) = (x - a_1)(x - a_2)...(x - a_n)$.

Proof. Let $g(x) = (x - u_1)(x - u_2)...(x - u_n)$. We know that g must have n roots $(u_1, ..., u_n)$.

Let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$.

$$\begin{aligned} h(x) &= f(x) - g(x) \\ &= x^n + a_{n-1}x^{n-1} + ... + x_1 x + a_0 - (x - u_1)...(x - u_n) \end{aligned} \tag{25}$$

We can see that h has degree *at most* $n - 1$ at the highest order terms will cancel.

If $h(x) \neq 0$, then it can only have $n - 1$ roots at most (as it is a degree at most $n - 1$ in mod p, which can only have $n - 1$ roots). But it must have n roots as u_i is a root of f and g.

So $h(x) = 0$ (it is the zero function), hence f can be factored like g, which is what we wanted. □

5.b)

$$f(x) = x^{p-1} - 1 \tag{26}$$

We know that $x^{p-1} = 0 \bmod p$ has $p - 1$ solutions to x, which is every number in $\mathbb{Z}/p\mathbb{Z}$. So we can write f as

$$f(x) = (x - 1)(x - 2)...(x - (p - 1)) \tag{27}$$

5.c)

Plug in $f(p) = f(0)$ for the same f as above.

$$f(0) = 0^{p-1} - 1 = -1 = \underbrace{(-1)(-2)...(p + 1)}_{(p-1)(p-2)...(1)} = (p - 1)! \bmod p \tag{28}$$

6)

6.a)

$$f(x) = x^3 - x \bmod 6 \tag{29}$$

$f(0) = 0, f(1) = 0, f(2) = 6 = 0, f(3) = 24 = 0, f(4) = 60 = 0, f(5) = 120 = 0.$

6.b)

$$f(x) = \prod_{k=0}^{m-1} (x - k) = x(x - 1)(x - 2)...(x - (m - 1)) \tag{30}$$

All $x \in \mathbb{Z}/m\mathbb{Z}$ are roots as seen in the factored form. Hence $d(m) \leq m$ as f is degree m and is identically zero for all $x \in \mathbb{Z}/m\mathbb{Z}$.

6.c)

$$g(x) = 0 \bmod p \forall x \in \mathbb{Z}/p\mathbb{Z} \tag{31}$$

We know that a polynomial of degree n has at most n solutions in mod p (from the theorem in class). But we cannot have more than n solutions because there are only n numbers! So $d(p) = p$.

6.d)

Want to show if $m' \mid m$ and if $f(x) = 0 \bmod m \forall x \in \mathbb{Z}/m\mathbb{Z}$, then $f(x) = 0 \bmod m' \forall x \in \mathbb{Z}/m'\mathbb{Z}$.

$m = m'k$ for some k.

$f(x) = ml \forall x \in \mathbb{Z}/m\mathbb{Z}$ for some l.

$f(x) = m'lk \forall x \in \mathbb{Z}/m'\mathbb{Z}$ for some k, l.

Hence $f(x) = 0 \bmod m'$ for all $x \in \mathbb{Z}/m'\mathbb{Z}$.

So $d(m') \leq d(m)$. If f is identically zero mod m, it is also identically zero mod m' for $m' \mid m$.

Let $m = 6, m' = 3$.

$f(x) = x^3 - x = 0 \bmod 6 \forall x \in \mathbb{Z}/6\mathbb{Z}$. This implies that $d(6) \leq 3$.

$f(x) = 0 \bmod 3$ for all $x \in \mathbb{Z}/3\mathbb{Z}$, hence $d(6) \geq 3$. Hence $3 \leq d(6) \leq 3 \implies d(6) = 3$.

6.e)

Show that $d(2p) = p$ for odd primes.

Suppose that $g(x) = 0 \bmod 2p \forall x \in \mathbb{Z}/2p\mathbb{Z}$.

Then $g(x) = 0 \bmod p$ for all$x \in \mathbb{Z}/p\mathbb{Z}$. This implies that $g(x) = x(x-1)(x-2)...(x-(p-1))$, which means that $d(2p)$ is bounded above by p (we have found a polynomial of degree p which is identically zero, so we have created an upper bound on $d(2p)$).

Let $m' = p, m = 2p$. Then $m' \mid m$. So

$$\begin{aligned} d(m') &\leq d(m) \\ d(p) &\leq d(2p) \\ p &\leq d(2p) \end{aligned} \tag{32}$$

So we have found the smallest possible degree of a polynomial to be identically zero mod $2p$.

Hence $p \leq d(2p) \leq p \implies d(2p) = p$.

6.f)

p is prime, f is a monic polynomial that is identically zero mod p^2.

Show f and f' are identically zero mod p.

We know that $f(x) = 0 \bmod p^2$ for all $x \in \mathbb{Z}/p^2\mathbb{Z}$. So $f'(x) = 0$ for all $x \in \mathbb{Z}/p\mathbb{Z}$ as we cannot have unique lifts to have all $f(x) = 0 \forall x \in \mathbb{Z}/p^2\mathbb{Z}$.

We also know that $f(x) = 0 \bmod p$ for all $x \in \mathbb{Z}/p\mathbb{Z}$ as we need all $x \in \mathbb{Z}/p\mathbb{Z}$ to satisfy $f(x) = 0 \bmod p$ (the "base" of our tree must have zeros for all x if we are to lift every single $x \in \mathbb{Z}/p\mathbb{Z}$).

6.g)

We want to show that there are no polynomials of degree 2 or 3 that are identically zero mod 4.

First check degree 2.

$$f(x) = x^2 + ax + b \tag{33}$$

We need $f(0) = 0$, so $b = 0$. We also need $f(1) = 0$, so $a = -1$.

Hence our $f(x) = x^2 - x$, but $f(2) = 4 - 2 = 2 \neq 0 \bmod 4$. So there is no degree 2 polynomial that is identically zero mod 4.

Now check degree 3.

$$g(x) = x^3 + ax^2 + bx + c \tag{34}$$

For $g(0) = 0$, we need $c = 0$. We need $g(1) = 0$, so $a + b = -1 \implies a = -b - 1$.

We need $g(2) = 0$, so

$$\begin{aligned} 8 + 4a + 2b &= 0 \\ 7 - 4(-b - 1) + 2b &= 0 \\ 6b &= 12 \\ b &= 2 \end{aligned} \tag{35}$$

Plugging $b = 2$ in we get that $a = -3$.

Hence our polynomial is $g(x) = x^3 - 3x^2 + 2x$, but $g(3) = 27 - 27 + 6 = 6 \neq 0 \bmod 4$.

We have shown that there is no polynomial of degree 2 or 3 that is identically 0 mod 4, so $d(4) = 4$.